车联网环境下基于重复博弈的恶意车辆节点检测机制 *

董文远 1†，朱　研 1，王永红 2，张光华 1

(1. 河北科技大学 信息科学与工程学院，石家庄 050018; 2. 承德石油高等专科学校 计算机与信息工程系，河北 承德 067000)

摘　要：针对车联网内部存在的虚假信息攻击，以及节点动态变化快及密集程度不同造成的恶意车辆节点检测机制效率低下，提出了一种基于重复博弈的恶意车辆节点检测机制。首先，根据车辆在信息交互中的行为建立重复博弈模型，并利用生成的节点收益计算出信任值与动态阈值，经二者比较，筛选出可疑的恶意车辆节点；其次，通过权值投票算法从可疑的恶意车辆节点中判定出恶意车辆节点；最后，从邻居列表中选取信任值最高的下一跳车辆节点进行合作。仿真和分析表明，与现有的相关机制相比，该机制提高了对虚假信息攻击的检测率，降低了误检率。

关键词：重复博弈；虚假信息攻击；投票算法；检测率；误检率

中图分类号：TP393.08　　doi: 10.19734/j.issn.1001-3695.2018.11.0829

Malicious vehicle node detection mechanism based on repeated game in VANET

Dong Wenyuan[1†], Zhu Yan[1], Wang Yonghong[2], Zhang Guanghua[1]

(1. *College of Information Science & Engineering*, *Hebei University of Science & Technology*, *Shijiazhuang* 050018, *China*; 2. *Dept. of Computer & Information Engineering*, *Chende Petroleum College*, *Chengde* Hebei 067000, *China*)

Abstract: In view of internet of vehicles within the false information attack, and node dynamic change fast and intensive different malicious nodes vehicle detection mechanism caused by inefficient, proposing a malicious nodes vehicle detection mechanism based on repeated game. First of all, according to the behavior of the vehicle in the information interaction establish the repeated game mode, and using the generated node income calculate the trust value and the dynamic threshold, by comparison, screening out the suspicious malicious vehicle nodes; Second, by weights of voting algorithm from suspected malicious nodes vehicles identify the malicious nodes vehicles; Finally, selecting the next-hop vehicle node with the highest trust value from the neighbor list to cooperate. Simulation and analysis show that compared with the existing mechanism, this mechanism improves the detection rate of false information to attack, reduces the error detection rate.

Key words: repeated game; false information attack; voting algorithm; detection rate; error detection rate

0　引言

车联网（Internet of vehicles，IoV）是物联网（Internet of things，IoT）在智慧城市交通领域中的具体应用，通过车辆网络动态的收集、分发和处理数据，利用无线通信方式共享信息，实现车与车、车与路、车与人、车与其他基础设施之间的信息交互，使汽车与城市网络相互连接[1]。然而，由于无线通信与车联网应用的高可靠性和高安全性之间存在着矛盾，车辆易受到恶意攻击，这就给车联网的安全带来了挑战。目前，从数据通信角度出发，可从车域网安全、车载自组网安全和车载移动互联网安全三个方面分析车联网面临的安全威胁[2~5]。

虚假信息攻击是车载自组网安全中面临的一种典型攻击，是借助 VANET 中节点之间共享开放信道的特点而实现的一种主动攻击方式[5]。在虚假信息攻击中，攻击者一旦捕获共享信道所在的频段，就可以冒充正常的车辆节点，向网络中散布虚假消息或窜改、延迟转发和丢弃接收后需要转发的信息，对道路交通和车主的人身安全及财产造成非常严重的影响。此外，车联网中车辆动态变化快及密集程度不同为引入高效的恶意车辆节点检测机制带来了极大的障碍[6~8]，很难将虚假信息攻击进行清除。以往对虚假信息攻击的检测研究大多数是基于无线传感器等静态网络，对车联网的研究很少。

本文在车联网中引入博弈论思想[9,10]，提出了一种基于重复博弈的恶意车辆节点检测机制 MDMBRV（malicious node detection mechanism based on repeated game in the VANET）。该机制利用博弈模型生成信任值与动态阈值，经二者比较筛选出可疑恶意车辆节点并将信息发送至基站，当基站收到可疑恶意车辆节点的信息后，将采取投票算法判定出恶意车辆节点；最后，通过节点优选算法选取下一跳车辆节点，促进节点之间的合作。对本文机制进行仿真，并与 MIDS（mixed intrusion detection scheme）[11]、AHP（Analytical hierarchy process）机制[12]在性能上进行比较。

1　相关工作

为了保证车联网的安全，同时又提高恶意车辆节点检测机制的检测效率。现有机制将博弈论思想引入到车联网中[13~20]，博弈论的优势在于能够根据每一阶段恶意节点的攻击方式选定合适的安全策略，从而降低恶意节点对网络造成的

收稿日期：2018-11-18；**修回日期：**2018-12-27　**基金项目：**国家自然科学基金资助项目（61572255）；国家重点研发计划资助项目（2016YFB0800703）；河北省高等学校科学技术研究项目（ZD2018236）

作者简介：董文远（1995-），男（通信作者），河北唐山人，硕士研究生，主要研究方向为物联网安全（957918257@qq.com）；朱研（1977-），男，讲师，硕士，主要研究方向为计算机应用；王永红（1978-），女，讲师，硕士，主要研究方向为网络安全；张光华（1979-），男，副教授，博士，主要研究方向为网络与信息安全.

危害。目前，运用博弈论的安全机制很多，大致可分为两类，一类是基于博弈的静态节点检测机制，另一类是基于博弈的动态节点检测机制。

在静态节点检测机制中，文献[13]考虑到无线传感器网络中信息安全、节点信誉和能源消耗三方面的矛盾，提出了一种基于双参数的多标准博弈入侵检测机制。该机制不仅阻止了最小能耗方面的信息泄露，而且将具有较高信誉的恶意节点从网络中删除，但不适用于节点信息不完整的动态场景；文献[14]提出了一种基于博弈论的攻击防御模型，该模型的关键特征是攻击者和防御者为了达到双方的最大收益，可以定期更改自己的策略，以提高 IDS 中 ESN 的能耗和检测率。然而，该理论模型只可应用于静态的嵌入场景；文献[15]提出了一种基于博弈论的无线传感器网络多层入侵检测框架，结合基于规范规则和轻量级神经网络的异常检测模块，来识别恶意传感器节点，不仅如此，该框架还在 IDS 和监控的传感器节点之间建立博弈模型，降低了 IDS 流量和网络能耗。当恶意节点较多时，该机制的检测效率较低；文献[16]在物联网中提出了一种基于博弈论的协同安全检测方法，通过对攻击者与防御者博弈后的分析，得出了在无限迭代次数（或有限迭代次数）完全一致（或不完全一致）的情况下协同博弈模型和纳什均衡之间的定量关系。该检测方法提高了恶意车辆节点的检测率和网络运行性能，但没有考虑节点动态变化对其造成的影响。综上所述，对于静态网络中恶意节点的检测和节点之间的合作给出了合理的建议，但均不适用于节点动态变化的网络。

而在动态节点检测机制中，文献[17]为延迟容忍网络提出了一种基于进化博弈的安全路由协议，该协议不需要任何基础设施支持，就可以阻止虫洞攻击、黑洞攻击、贪婪攻击、窜改攻击等恶意行为对网络造成的威胁，但该协议只适用于延迟容忍网络，对其他网络的应用正在研究过程中；文献[18]在车联网中提出了一种基于博弈论的网络信任模型，运用多数意见、中介中心值和节点密度这三个参数，使节点能够更好地了解网络及其周围环境，有效的防止了恶意行为的发生，但该方案并没有解决通信的可靠性问题；文献[19]针对移动自组织网，提出了一种多包协同入侵检测的博弈理论模型。该模型检测准确率高且时延小，但是计算量复杂、能耗大；文献[20]由于对隐私泄露和资源成本问题的担忧，提出了一种基于进化博弈的合作入侵检测激励机制，该机制研究一个博弈算法来最大化节点效用，促进了节点之间的合作，但是对于恶意车辆节点的检测效率并不高。

上述基于博弈论的检测机制中，无论是针对于静态节点还是动态节点，均没有同时考虑车联网中节点动态变化及密集程度造成的问题。为此,本文提出了基于重复博弈的恶意车辆节点检测机制，分析节点之间的博弈过程，生成节点的信任值与动态阈值，并根据本文规则将这些参数进行处理，从而识别出网络中的恶意车辆节点，确保在开销和能耗允许的情况下提高恶意车辆节点检测率，降低误检率。

2 基于重复博弈的恶意车辆节点检测机制研究

为了提高恶意车辆节点检测机制的检测效率、防止恶意车辆节点对其他节点进行虚假信息攻击,如图 1 所示，本方案可从五个方面进行分析：a)根据重复博弈理论将车辆间的信息交互看做是一个多次博弈过程，建立阶段重复博弈模型，求出车辆节点的收益，并将该信息发送至每一区域的基站 S（本文假设基站 S 完全可信）；b)利用转换因子将车辆节点收益转换为信任值与动态阈值；c)基站 S 将车辆节点信任值与动态阈值进行比较，选出可疑恶意车辆节点;d)考虑到车辆密集程度不同，选取多车辆权值投票算法或单车辆权值投票算法判定出恶意车辆节点，并将该车辆节点信息进行广播，以便于其他车辆将该车辆节点信息在邻居列表中剔除;f)利用节点优选合作算法选出下一跳车辆节点。

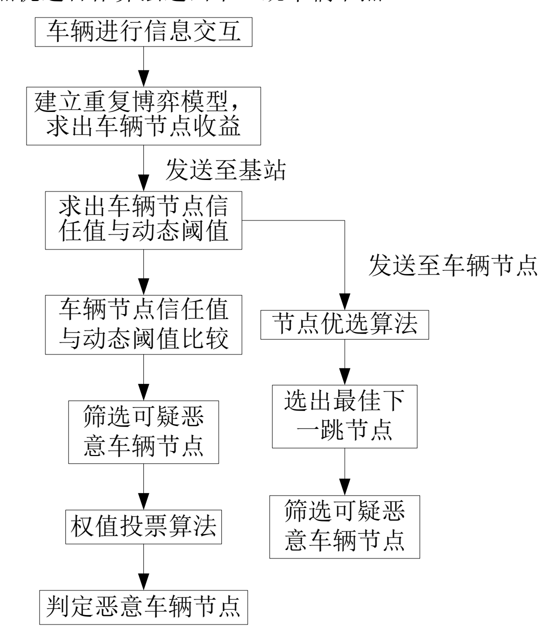


图 1 MDMBRV 的工作流程

Fig. 1 Workflow of MDMBRV

2.1 重复博弈模型

2.1.1 网络模型定义

恶意车辆节点与正常车辆节点重复博弈模型包括四个方面，分别是参与节点、行动空间、收益情况和重复博弈次数。定义如下：

定义 1 参与节点是指一个博弈中参与行动的主体。该模型参与节点的类型空间为$\{m, n\}$，m 代表进行虚假信息攻击的恶意车辆节点，能对邻居节点造成威胁和破坏。n 代表正常运行的车辆节点，不会对邻居车辆造成任何威胁。

定义 2 行动空间。行动是指参与节点在博弈过程中选取的相关策略。本文考虑到恶意车辆节点的两种行动方案，分别为进行虚假信息攻击 M_1 和正常运行 M_2，记为 $M=(M_1,M_2)$。同样，正常车辆节点也有两种行动方案，分别为开启恶意车辆节点检测机制进行防御 N_1 和正常运行 N_2，记为 $N=(N_1,N_2)$。将 M 和 N 两两组合，便可得到恶意车辆节点与正常车辆节点的所有行动组合矩阵 G，如式(1)所示。

$$G=\begin{bmatrix}(M_1,N_1) & (M_1,N_2)\\(M_1,N_2) & (M_2,N_2)\end{bmatrix} \tag{1}$$

定义 3 收益情况是指博弈模型中参与节点根据自身的类型选取相关行动所获收益。本文假设 U_m 为恶意车辆节点每一阶段博弈所获收益。U_n 为正常车辆节点每一阶段博弈所获收益。

定义 4 重复博弈次数。本文博弈模型在进行博弈过程中无法确定博弈何时终止、博弈次数为多少，因此将博弈过程看为随机结束重复博弈，。

2.1.2 博弈模型的建立

为了方便计算，本文只对车联网中恶意车辆节点与正常车辆节点的博弈过程进行分析，正常车辆节点之间与恶意车辆节点之间的博弈分析过程忽略不计。

为了确定恶意车辆节点与正常车辆节点的收益函数，需要对一些符号进行定义，如表 1 所示。

表 1 重复博弈模型符号定义

Table 1 Repeated game model symbol definition

符号	定义
$C_i(t)$	恶意车辆节点进行虚假信息攻击所获收益
$V_i(t)$	恶意车辆节点进行虚假信息攻击所付出代价
$Q_i(t)$	正常车辆节点进行防御所获收益
$P_i(t)$	正常车辆节点进行防御所付出代价
$U(t)$	车辆节点正常运行所获收益

通过分析重复博弈模型的博弈过程，可以得到恶意车辆节点与正常车辆节点阶段博弈的收益函数，如式(2)(3)所示。

$$U(m)=\begin{bmatrix}-V_i(t) & C_i(t)-V_i(t)\\ U(t) & U(t)\end{bmatrix} \tag{2}$$

$$U(n)=\begin{bmatrix}-Q_i(t)-P_i(t) & -P_i(t)\\ U(t) & U(t)\end{bmatrix} \tag{3}$$

为了节省网络资源，本文规定节点最高收益指标为 μ，当博弈中一个节点的收益达到最高指标 μ，博弈过程结束，重复博弈模型的算法如算法 1 所示。

算法 1 重复博弈模型算法

输入：最高收益为 μ。

1 节点 *A* 与节点 *B* 进行博弈。

2 计算每一阶段博弈 *A* 与 *B* 的收益，并求出其总体收益 *U*（*A*）和 *U*（*B*）。

3 if （$U(A)>\mu$ or $U(B)>\mu$）then

博弈过程结束；

end if

4 else

博弈继续进行，执行步骤 1、2，直到满足步骤 3 为止。

5 end

2.2 收益与信任值转换

因为恶意车辆节点与正常车辆节点在博弈过程中为获取更多的收益而采取不同的策略去进行博弈，为了对二者类型进行区分，本机制假定一个转换因子 δ，将节点收益转换为节点信任值，如果为恶意行为的收益，节点信任值将根据 δ 与节点收益做差，如果为正常行为的收益，节点信任值将根据 δ 与节点收益做和，当收益为负值时，节点信任值用 0 表示。最后经过计算求出节点信任值 T_i，并将该节点信息发送至基站 *S*。节点收益与信任值的转换方法如算法 2 所示。

算法 2 收益与信任值转换算法

输入：节点信任值 T_i。

输出：博弈后的节点信任值 T_i。

通过分析，判定节点采取的行动为恶意行为还是正常行为，恶意行为用 1 表示，正常行为用 2 表示，节点为 *N*。

```
if (N=1)
    if (U<0)
        T_i = T_i + 0;
    else
        T_i = T_i − δU;
    end if
    if (N=2)
        if (U<0)
            T_i = T_i + 0;
        else
            T_i = T_i + δU;
        end if
end
```

2.3 可疑恶意车辆节点选取

为准确的选取产生虚假信息攻击的可疑恶意车辆节点，需要设置合适的动态阈值。本文采取全局阈值求解算法来解决这个问题。详细算法流程如下所示：

a)设定参数 ε_0，并根据节点的信任值选择一个初始的估计阈值 ε_1。

b)估计阈值 ε_1 将节点分割为两部分 N_1 和 N_2， N_1 为信任值大于 ε_1 的节点， N_2 为信任值小于 ε_1 的节点。

c)计算 N_1 和 N_2 中所有节点的平均信任值 λ_1 和 λ_2，以及新的阈值 $\varepsilon_2=(\lambda_1+\lambda_2)/2$。

d)如果 $|\varepsilon_1-\varepsilon_2|<\varepsilon_0$ 则推出 ε_2 为最优动态阈值；否则，将 ε_2 赋值给 ε_1，重复步骤 b)~d)直到获取最优阈值 ε。

由算法 1 和 2 可知节点在博弈过程中存在相应的信任值 T_i，又根据全局阈值法求出了节点的最优动态阈值 ε。之后将得到的节点信任值 T_i 与动态阈值 ε 进行比较，判定节点 *N* 是否为可疑恶意车辆节点，即

当 $T_i>\varepsilon$ 时，节点 N 为可疑恶意车辆节点。

当 $T_i<\varepsilon$ 时，节点 N 为可疑正常车辆节点。

当 $T_i=\varepsilon$ 时，等待下一次博弈检测结果。

算法 3 可疑恶意车辆节点选取算法

输入：节点信任值 T_i 和动态阈值 ε。

输出：节点为可疑恶意车辆节点还是可疑正常车辆节点的选取结果。

```
if（T_i > ε）
  为可疑正常车辆节点；
end if
if（T_i < ε）
  为可疑恶意车辆节点；
end if
if（T_i = ε）
  继续进行博弈检测；
end if
end
```

2.4 恶意车辆节点判决与剔除

在车联网中，车辆之间距离和链路质量不同，单一车辆节点的判定结果可能出现误差，需要采用多车辆节点投票算法避免发生此类问题，当大多数车辆判定某车辆节点为可疑的恶意节点时，则该节点可被判定为恶意车辆节点。

在实际投票过程中，考虑到车辆可信程度不同，需要引入权重这个概念，提高判定结果的准确度。由式（4）可求出本文节点权重，权重越大，节点在投票中的影响力越大，权重越小，节点在投票中的影响力越小。

$$W_i=\frac{T_i}{T_1+T_2+T_3+\cdots+T_{i-1}+T_i} \tag{4}$$

同时，车辆密集程度不同降低了节点投票算法的稳定性与可靠性。为此，本文在基于 Boyer-Moore 投票算法基础上[21]引入式(4)中的节点权重，提出了两类算法，一类是适用于节点密集的多车辆权值投票算法，如算法 4 所示；另一类是适用于节点稀疏的单车辆权值投票算法，如算法 5 所示。

算法 4 多车辆权值投票算法

输入：起始投票数 C_{sum}。

输出：总投票数 C_{sum}。

1 建立与节点 *N* 进行博弈的邻居列表集合 $(a_1,a_2,a_3,\cdots,a_i)$，该邻居列表集合 a_i 为对节点 N 是恶意车辆节点还是正常车辆节点的判断，0 代表为可疑正常车辆节点，1 代表为可疑恶意车辆节点。

2 根据信任值求出邻居列表中每一车辆节点的权重 W_i。

for $(i=1, j=n; i<j; i++)$

```
    if  (a_i = 0)
        C_sum = C_sum + 1*W_i ;
    end if
    if  (a_i = 1)
        C_sum = C_sum - 1*W_i ;
    end if
end
```

算法 5　单车辆权值投票算法

```
重复算法 4 中的步骤 1、2，求出每一车辆节点的权重 W_i 。
将每一个节点的权重进行比较，求出最大权重的节点 a_i 。
if  a_i 为最大权重节点 then
    权重为 a_i 的节点对节点 n 的判定为正确判定结果；
end if
end
```

基站进行广播，警告周边节点当存在其他下一跳节点时，忽略该节点。当不存在其他下一跳节点时，为保证链路稳定性，对转发信息进行标记，并告知目的节点对该信息准确性进行分析。

在本文研究中，采取多车辆权值投票算法判定 N 是否为恶意车辆节点取决于参与投票车辆节点的总投票数 C_{sum} 。当邻居车辆节点判定 N 为恶意车辆节点时投票数减少，N 为正常车辆节点时投票数增多，总投票数 C_{sum} 越大证明 N 为正常车辆节点的准确率越高，反之则越小。

类似地

当 $C_{sum} > 0$ 时，说明节点大多数投票认为 N 为正常车辆节点，则判断 N 且正常车辆节点；

当 $C_{sum} < 0$ 时，说明节点大多数投票认为 N 为恶意车辆节点，则判断 N 为恶意车辆节点；

当 $C_{sum} = 0$ 时，无法判断 N 为正常车辆节点还是恶意车辆节点，等待下一次投票。

具体过程如算法 6 所示。

算法 6　恶意车辆节点判决

```
输入：总投票数 C。
判断节点密集程度。
if 节点密集程度较大
    执行算法 4;
    if  (C_sum > 0)  then
        n 为正常车辆节点;
    end if
    if  (C_sum < 0)  then
        n 为恶意车辆节点，基站进行广播，请求周边节点将该节点从邻居列表中剔除;
    end if
    if  (C_sum = 0)  then
        等待下一次投票;
    end if
  else
    执行算法 5;
  end if
end
```

2.5　节点优选合作算法

基于上述模型和算法，已求出各车辆节点的信任值与权重，并将恶意车辆节点剔除出了网络。为进一步提高传输信息的可靠性与安全性，保证节点之间的合作效率，提出了一种节点优选合作算法，该算法能够为节点优先选择邻居列表中信任值最高的下一跳节点进行信息传输。具体节点选取流程如下所示：

a)请求节点将邻居列表中下一跳节点的信任值从高到低进行排序，选取信任值最高的下一跳节点为请求节点合作对象，并发送请求信息。

b)下一跳节点收到请求节点的请求信息后，将自身情况信息（包括位置、速度、周边车辆密集程度等）告知于请求节点，询问是否接收信息并进行传输。

c)根据 a)b)将信息一直传输下去，直到信息到达目的节点为止。

3　仿真实验与分析

3.1　环境设置

本文使用的交通仿真工具是 NS-2[22]，车辆交通运行场景生成工具是 SUMO[23].NS-2 是 UC Berkeley 开发的离散事件网络模拟器，由 C++语言定义，通过 Otcl 脚本语言提供仿真接口，支持 VANET 路由协议和 802.11MAC 的实现。SUMO 是一款开源微观交通仿真软件，通过使用 MOVE 配置得到所需的路网和路径等 XML 文件。本文模拟道路交通复杂、车辆密集程度不同的某城市街道场景，在 $20km*20km$ 的城市里生成接近真实车辆驾驶的车辆位置、速度、密度等数据的 trace 文件，并载入 NS-2 仿真模拟器，仿真实验参数如表 2 所示。

表 2　仿真参数设置

Table 2　Simulation parameter Settings

参数	参数值
仿真范围	$20km*20km$
节点速度	$30\text{-}100km/h$
节点数量	200
通信半径	$1000m$
MAC 协议	802.11P
数据包传递速率	$1Kbit/s$
攻击类型	虚假信息攻击
车辆密度单位	$180vel \cdot km^{-1} \cdot ln^{-1}$

3.2　实验结果和对比分析

为了验证本方案的有效性，定义了检测率和误检率两个评价标准，检测率是指成功检测出恶意车辆节点的数量与网络中存在的恶意车辆节点数量之比，误检率是指正常车辆节点被误检为恶意车辆节点的比例。同时，为了提高本机制的准确性，将实验进行多次仿真求出其平均值。当恶意车辆节点数量不同时，MDMBRV 对虚假信息攻击的检测率和误检率如图 2、3 所示。

图 2 是 MDMBRV、MIDS 与 AHP 机制在检测率方面的对比图，可以看出随着恶意车辆节点数量的增加，三个机制的检测率略有下降的趋势，MIDS 机制下降幅度最大，其次为 AHP 机制，MDMBRV 机制下降幅度最小。与 MIDS 和 AHP 机制相比，MDMBRV 能维持较高的恶意车辆节点检测率。主要原因是 MDMBRV 采用多车辆投票算法，使用周边车辆都可以对可疑节点进行判决，提高了恶意车辆节点检测的准确性。

图 3 是 MDMBRV、MIDS 与 AHP 机制在误检率方面的对比图，可以看出随着恶意车辆节点比例的上升，MDMBRV、MIDS 与 AHP 的误检率逐步提高。相对于 MIDS 与 AHP 机制，MDMBRV 仍保持着较低的误检率。主要是因为本机制引入的全局阈值法能随着环境的变化动态的实时调整动态阈值。

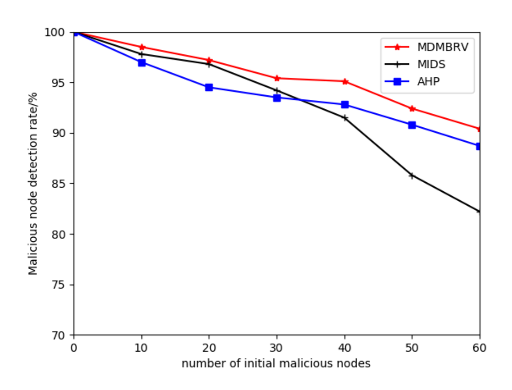


图 2　检测率随初始恶意车辆节点数目的变化情况

Fig. 2　Detection rate with the change of initial malicious traffic node number

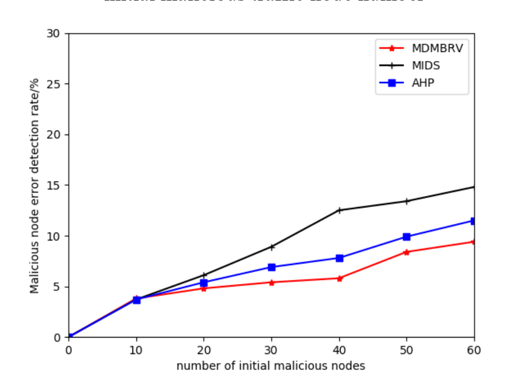


图 3　误检率随初始恶意车辆节点数目的变化情况

Fig. 3　Error detection rate with the change of initial malicious traffic node number

当节点动态变化时，节点密度也在变化，图 4、5 为不同车辆密度下 MDMBRV 对虚假信息的检测率和误检率。

从图 4 中可以看出当车辆密度增加时，三种检测机制的检测率都有所上升。本文机制检测率在车辆密度为 $20vel\cdot km^{-1}\cdot ln^{-1}$ 到 $180vel\cdot km^{-1}\cdot ln^{-1}$ 之间时一直高于 MIDS 与 AHP 机制，并在车辆密度为 $180vel\cdot km^{-1}\cdot ln^{-1}$ 的情况下，检测率高达 96.5%。主要是因为车辆密度的上升增加了可疑车辆周边的邻居车辆，提高了投票算法的准确性。

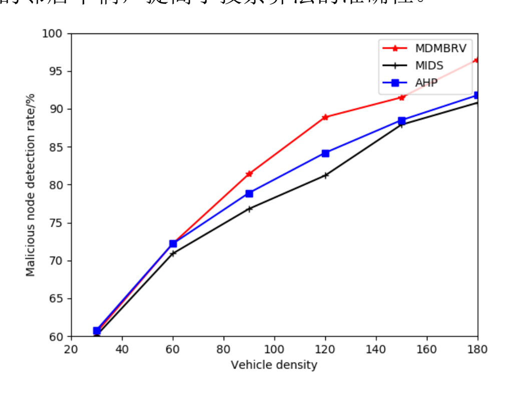


图 4　检测率随车辆密度的变化情况

Fig. 4　Detection rate with the change of vehicle density

图 5 显示随着车辆密度的上升，MIDS 与 AHP 机制误检率上升幅度明显，而 MDMBRV 机制误检率起始虽有所上升，但在 $120vel\cdot km^{-1}\cdot ln^{-1}$ 之后略有下降趋势，总的来说保持着平稳状态，并且低于 MIDS 与 AHP 机制。相较于 MIDS 与 AHP 检测机制，本机制不易受到车辆密度干扰，有更好的误检率。主要原因是根据车辆密度的不同，可以适当地选择多车辆权值投票算法和单车辆权值投票算法进行运算。

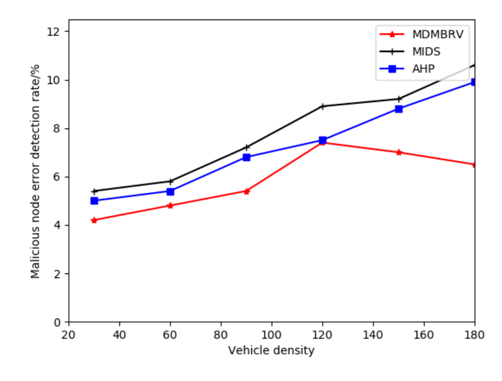


图 5　误检率随车辆密度的变化情况

Fig. 5　Error detection rate with the change of vehicle density

为了分析车辆密度对网络开销的影响，设置了车辆速度为 30 *km/h*，车辆密度不同的场景。随机选取两个进行虚假信息攻击的恶意车辆，观测不同场景下，MDMBRV 识别虚假信息攻击过程的网络开销。如图 6 所示，随着车辆密度的增加，两种机制网络开销逐渐上升。MDMBRV 网络开销上升趋势明显，并且高于 MIDS 检测机制。这是因为车辆密度的上升提高了 MDMBRV 机制节点之间的博弈过程，从而产生了更大的网络开销。

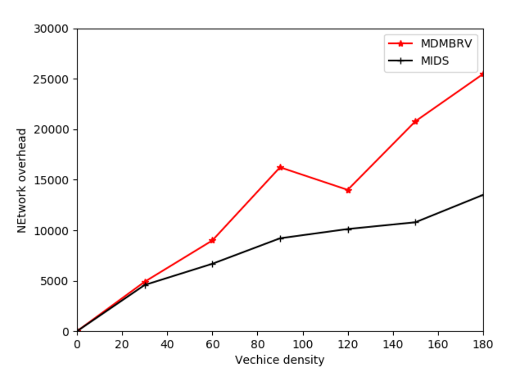


图 6　车辆密度对网络开销的影响

Fig. 6　Vehicle density on the influence of network overhead

4　结束语

本文为了提高车联网中恶意车辆节点检测机制的检测效率，避免车辆受到虚假信息攻击，提出了基于重复博弈的恶意车辆节点检测机制，将重复博弈与投票算法相结合，通过分析节点间的博弈行为和采取投票算法识别出车联网中的恶意车辆节点，最后，为了促进节点之间的合作，选取最优下一跳节点进行信息传递。此外，从检测率、误检率和通信开销三个方面验证了 MDMBRV 的有效性。下一步将在目前的 MDMBRV 基础上，降低网络开销，并研究 Sybil、DoS 等攻击行为的恶意车辆节点检测方法。

参考文献：

[1] Xu Wenchao, Zhou Haibo, Cheng Nan, *et al.* Internet of Vehicles in Big Data Era [J]. IEEE/CAA Journal of Automatica Sinica, 2018, 5(1): 19-35.

[2] Chen Jiacheng, Zhou Haibo, Zhang Ning, *et al.* Service-oriented dynamic connection management for software-defined Internet of vehicles [J]. IEEE Trans on Intelligent, Transportation System,2017,18(10):2826–2837.

[3] Yadav K, Vijayakumar P. VANET and its security aspects: a review [J]. Indian Journal of Science Technology, 2016, 9(44): 59-64.

[4] Muhammad A, Elyes B, Wassim Z, *et al.* Security in intelligent transport systems for smart cities: from theory to practice [J]. Sensors, 2016, 16(6): 879.

[5] Li Fujuan, Wang Qun, Qian Huanyan, *et al.* Survey on security threats of Internet of vehicles [J]. Application of Electronic Technique, 2017, 43(5): 29-33, 37.

[6] Roshan J, Preetam S. Detection of malicious node and development of routing strategy in VANET [C]//Proc of International Conference on Signal Processing and integrated Networks.2016: 472-476.

[7] Subba B, Biswas S, Karmakar S. A game theory based multi layered intrusion detection framework for VANET [J]. Future Generation Computer Systems, 2018, 82(5): 12-28.

[8] Jared O. A Distributed reputation scheme for situation awareness in vehicular Ad hoc networks (VANETs) [C]//Proc of IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support.2016: 1-5.

[9] Liang Xiannuan, Xiao Yang. Game theory for network security [J]. IEEE Communications Surveys&Tutorials, 2013, 15 (1): 472-486.

[10] Abdalzaher M, Seddik K, Elsabrouty M, et al. Game theory meets wireless sensor networks security requirements and threats mitigation: a survey [J]. Sensors, 2016, 16 (7): 1003.

[11] 李春彦，刘怡良，王良民．车载自组网基于交通场景的入侵行为检测机制 [J]. 山东大学学报, 2014, 44(1): 29-34. (Li Chunyan, Liu Yiliang, Wang Liangmin. Intrusion detection scheme based on traffic scenarios in vehicular ad hoc networks [J]. Journal of Shandong University, 2014, 44(1): 29-34.)

[12] Saraswat D, Chaurasia B. AHP Based Trust Model in VANETs [C]//Proc of the 5th International Conference on Computational Intelligence and Communication Networks.2013: 27-29.

[13] Guan Sanghai, Wang Jingjing, Jiang Chunxiao, *et al.* Intrusion detection for wireless sensor networks: a multi-criteria game approach [C]//Proc of IEEE Wireless Communications and Networking Conference .2018: 1-6.

[14] Wang Kun, Du Miao, Yang Dejun, *et al.* Game-theory-based active defense for intrusion detection in cyber-physical embedded systems [J]. ACM Trans on Embedded Computing Systems, 2016, 16(1): 1-21.

[15] Subba B, Biswas S, Karmakar S. A game theory based multi layered intrusion detection framework for wireless sensor networks [J]. International Journal of Wireless Information Networks, 2018(4): 1-23.

[16] Wu Hao, Wang Wei, A game theory based collaborative security detection method for Internet of things systems [C]. IEEE Trans on Information Forensics&Security, 2018, 13(6): 1432-1445.

[17] Guo Hang, Wang Xingwei, Cheng Hui, *et al.* A routing defense mechanism using evolutionary game theory for delay tolerant networks [J]. Applied Soft Computing Archive, 2016, 38(C): 469-476.

[18] Mehdi M, Raza I, Hussain S.A game theory based trust model for vehicular Ad hoc networks [J].Computer *Networks*, 2017, 121(7): 152-172..

[19] Purbita C, Koushik M, Anurag D. A game theoretic model to detect cooperative intrusion over multiple packets [C]//Artificial Intelligence and Evolutionary Computations in Engineering Systems.2016: 895-907.

[20] Guo Yunchuan, Zhang Han, Zhang Lingcui, et al, Incentive mechanism for cooperative intrusion detection: an evolutionary game approach [C]//Proc of International Conference on Computational Science.2018: 83-97.

[21] Rahim R, Ahmar A, Ardyanti, *et al.* Visual Approach of Searching Process using Boyer-Moore Algorithm [J]//Proc of International Conference on Information and Communication Technology. 2017: 1-5.

[22] Henderson T, Network simulater 2. 31 [EB/OL].(2007-03-10) [2018-11-08]. http://mailman.isi.edu/pipermail/ns-developers/2007-March/002931. html.

[23] Krajzewicz D, Hertkorn G, Rossel C, *et al.* SUMO (simulation of urban mobility): an open-source traffic simulation [C]//Proc of the 4th Middle East Symposium on Simulation and Modelling. 2002: 183-187.